

Notice of Allowability

Application No.

10/617,642

Examiner

Minh Dinh

Applicant(s)

PARK ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to after final amendment filed 7/18/07.
2. ☒ The allowed claim(s) is/are 4,6-10,12,14,15,17-22,24-26 and 28-32.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

DETAILED ACTION

Response to Amendment

1. This action is in response to the after final amendment filed 7/18/07. Claims 4, 6-8, 12, 15, 17, 22 and 24-25 have been amended; claims 1-3, 13, 16, 23 and 27 have been cancelled.

Allowable Subject Matter

2. Claims 4, 6-10, 12, 14-15, 17-22, 24-26 and 28-32 are allowed.
3. The following is an examiner's statement of reasons for allowance. The present invention is directed to methods for generating a key for data encryption. Independent claim 1 identifies the uniquely distinct feature "permutating the intermediate value by exchanging a selected number of bits of the IV value with an equal number of other bits of the IV value and outputting a result of the bitwise XOR operation and the exchange of the bits as a value that is bit shifted". Independent claim 12 identifies the uniquely distinct feature "differently processing the first secret key comprises performing a bitwise shift of the first secret key in instances in which the key change information has repeated". Independent claims 15 and 25 identify the uniquely distinct feature "wherein generating the key for data encryption comprises differently processing the second temporary key to generate the

key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated". Independent claim 22 identifies the uniquely distinct feature "determining if the data is originally encrypted in accordance with a predetermined encryption technique; and decrypting the data if the data is originally encrypted in accordance with the predetermined encryption technique, prior to encrypting the data transmitted via the communication network with the final key". The closest prior art, Housley et al. "Alternate Temporal Key Hash" and Housley et al. "Temporal Key Hash", disclose an encryption method for in wireless LANs. Specifically, Housley discloses a two-phase process for generating an encryption key using a MAC address and an initialization vector. However, Housley, either alone or in combination, does not teach the specific features mentioned above. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claims are therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays,

should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/617,642
Art Unit: 2132

Page 5

/MD/
Minh Dinh
Examiner
Art Unit 2132

7/26/07


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100